Collapsing Resource Domains

Most current Exchange messaging designs place Exchange on member servers. To save money, All-Terrain decided to create a dedicated messaging resource domain and put Exchange servers on BDCs and even the PDC. They also put the Exchange service account (**EXservice**) in the EXCHANGE resource domain instead of in ACCOUNTS. This last step makes the upgrade to Windows 2000 more challenging because as soon as the resource domain containing the Exchange service account is collapsed, all Exchange servers residing in the ACCOUNTS domain will have services that reference an account (EXCHANGE\Exservice) that no longer exists.

You have two options for maintaining Exchange functionality while upgrading:

- Keep the EXCHANGE resource domain intact and just upgrade it to Windows 2000. Then when you upgrade the Exchange servers to Exchange 2000, the service account will default to the local system account instead of a domain account and you can move the servers freely among any Windows 2000 domain in the forest. When you have them where you want them, you can collapse the EXCHANGE resource domain. *This is the safest approach*.
- Change permissions on the Exchange Org, Site, Configuration and Schema containers and all the Exchange services from EXCHANGE\EXservice to ACCOUNTS\EXservice. This is a good solution for small companies with one Exchange server per site. Large Exchange installations can also use it, but Microsoft does not support it unless the Exchange databases are backed up, the Exchange server software is reinstalled with the new service account and the Exchange databases are restored. *A less-safe approach:* it requires careful planning and good backups.

All-Terrain used a hybrid approach that appears to work (read about it in the “From the Trenches” section below) but option 1 is highly recommended unless your Exchange servers were installed using a service account from a domain other than the domain they are running in. **NOTE:** If you decide to use option 2 and you have Exchange installed on the PDC in your resource domain, you should add another BDC to the domain and promote it to the PDC role for contingency purposes. Before you can collapse Exchange servers into an OU you must first demote them to member servers; once you do that, any accounts that were in the SAM database of the domain being collapsed are gone unless the PDC role has been assigned to a non-Exchange server. You should keep the PDC on-line until all Exchange servers have been relocated.

From the Trenches: Collapsing an Exchange Resource Domain

Many companies upgrade to Windows 2000 to simplify domain administration and save on hardware costs by reducing the number of servers required. At one of my customer sites we recently collapsed the messaging resource domain, eliminating a PDC and a BDC in the process. That's a good deal, but this is not an operation to be taken lightly—if you don't do it correctly Exchange services may not start and you will be prevented from performing Exchange Administration until you rebuild your Exchange server(s).

Still willing to give it a try? I’ve outlined the procedure I used. You will have to adapt it to your situation but the principles are the same.

What We Started With

We started with a Windows 2000 root domain (**accounts.allterrain.com**) and a Windows NT 4.0 resource domain (**EXCHANGE**). The Windows 2000 domain retained ACCOUNTS as the NetBios name and I established a one-way trust between the two domains (EXCHANGE trusts ACCOUNTS). The EXCHANGE domain contained a PDC and 7 BDCs, 6 of which had Exchange installed.

The Exchange servers represent three Exchange sites (HOMEOFFICE, STORES, and LOGISTICS). All Exchange servers were originally installed using a service account from the Exchange resource domain and not the ACCOUNTS domain. This is significant: if they had been installed with an account from the ACCOUNTS domain we would not have had any problems collapsing the domain.

Our Objective

We wanted to reclaim two servers and simplify domain administration by collapsing the EXCHANGE resource domain into an Exchange OU inside of ACCOUNTS, while maintaining e-mail connectivity, administrative access to Exchange, and changing the Exchange service account and password.

The Problem

To collapse the Exchange resource domain we had to convert all the Exchange servers from BDCs to Windows 2000 member servers, join them to the ACCOUNTS domain, and then turn off the PDC and BDC for the EXCHANGE domain. The problem is that once the PDC in the EXCHANGE resource domain is turned off, Exchange Administrator permissions and Exchange services both reference an account from a domain that no longer exists so you cannot administer the site or start the services. If you edit the services so that they start with an account from ACCOUNTS, Exchange services will start but you no longer have access the Exchange Admin program—to get back in, you have to reinstall Exchange.

How We Did It

I used the steps below to collapse the domain while maintaining message delivery during preparation. We added the Exchange Administrator accounts and modified the Exchange services during weeknights, and collapsed the domain over a weekend because it required shutting the Exchange system down for about eight hours.

Please keep in mind that we walked through the entire process in a lab before ever touching a production Exchange server. This is a *high-risk* procedure and you must have a proven backup of all Exchange servers in your resource domain before you start in on it.

That being said, here are the steps we followed:

1. Created an Exchange service account in the ACCOUNTS domain (ACCOUNTS\ex2000). **Note:** The target domain service account name does not match the source domain service account name.

2. Opened the Exchange Administrator program on each Exchange server and assigned ACCOUNTS\Administrator and ACCOUNTS\ex2000 Service Account Admin permissions at the Org, Site, and Configuration container levels. **Note:** I did not do this in RAW mode.

3. Opened the Exchange Administrator program on each Exchange server in RAW mode (**\exchsrvr\bin\admin.exe /r**) and used this procedure to add ACCOUNTS\ex2000 to the schema object:
    - To view the raw directory, select the **View** menu, then select **Raw Directory**. (The **Schema** object is added in the left-hand pane of the **Exchange Administrator** window.)
    - Open the **Schema Properties** dialog box.
    - Select the **Schema** object.
    - From the **File** menu, select **Raw Properties...** to display the **Schema Properties** dialog box.
    - Add the new Service Account to the **NT-Security-Descriptor** object.
    - From the **Object attributes** list box, select the **NT-Security-Descriptor** object.
    - Click **Editor...**.to display the **Attribute Editor Selection** dialog box.
    - From the **Editor type** list box, select **NT security descriptor** and click **OK** to display the **NT-Security-Descriptor Properties** dialog box.
    - Click **Add....** to display the **Add Users and Groups** dialog box.

    - From the **List Names From** drop-down list box, select the domain where you created the new Service Account.
    - From the **Names** list box, select the new Service Account and click **Add**. (The new Service Account appears in the **Add Names** box.)
    - Click **OK**.
    - From the **Windows NT accounts with permissions** list box, select the new Service Account.
    - From the **Roles** drop-down list box, select **Service Account Admin**.
    - Click **OK**.
    - Click **OK** to close the **Schema Properties** dialog box.
    - Close Exchange Administrator.
4. Edited each Exchange service on each Exchange server so that they started up with ACCOUNTS\ex2000 instead of EXCHANGE\exservice.
5. Rebooted to make sure all the services still worked. They did.
6. Created a zone on **corp.allterrain.com** called **exchange.corp.allterrain.com** and enabled updates.
7. Upgraded the EXCHANGE domain PDC (EXCH-PDC) to a Windows 2000 child domain DC, keeping the down-level domain name of EXCHANGE. Now I have a child domain called **exchange.corp.allterrain.com**, which is running in mixed mode. The PDC is Windows 2000 RC2 and the BDCs are still Windows NT 4.0. **Note:** All Exchange services still start at this point and I can still send messages in both directions.
8. Upgraded EXCH-BDC to a Windows 2000 member server in the EXCHANGE domain. **Note:** I tried to join the member server directly into the ACCOUNTS domain, but when you cancel out of DCPROMO the option to join a different domain is greyed out. I got around this by running DCPROMO, selecting **Leave as a member server**.
9. Joined EXCH-BDC to a workgroup and rebooted. **Note:** I don't think this is necessary but I did it anyway just in case.
10. Joined EXCH-BDC to the ACCOUNTS domain.
11. Added ACCOUNTS\Administrator and ACCOUNTS\ex2000 to the Adminstrators local group on EXCH-BDC.
12. Gave ACCOUNTS\ex2000 "Logon Locally, Logon as a Service, Act as part of the Operating System and Restore Files and Directories" permissions to EXCH-BDC.
13. Ran SECEDIT /refreshpolicy MACHINE_POLICY and SECEDIT /refreshpolicy USER_POLICY to force the application of the additional rights. Exchange still worked and I could modify permissions on EXCH-BDC when logged in as ACCOUNTS\Adminsitrator. **Note:** During this entire process the Exchange services on EXCH-BDC were not available.
14. Started Exchange services on EXCH-BDC (STORES site) and it came right up. I could send and receive mail with (HOMEOFFICE) site, which at this point was still on a Windows 2000 DC in the EXCHANGE domain. We had to recreate the MAPI profile on EXCH-BDC after the move because the account associated with it remained in the EXCHANGE resource domain and could no longer be resolved to a valid account name in the ACCOUNTS domain. As long as the alias name associated with a particular MAPI profile can still be resolved, upgrading the server that Exchange 5.5 is installed on and moving it to a different domain should not affect existing MAPI profiles.
15. Repeated steps 8 through 14 on the remaining BDCs and member servers in the EXCHANGE resource domain.

16. Ran DCPROMO on the PDC (EXCH-PDC) to demote it to a member server. Since it was the last DC in the domain, it automatically became a member of "workgroup." I changed the domain to "ACCOUNTS" and rebooted. **Note:** I did NOT stop EXCH-BDC Exchange services while EXCH-PDC was being upgraded (contrary to some Knowledge Base articles) because I didn't see why it would be necessary. It turns out it's not.
17. Added ACCOUNTS\Administrator and ACCOUNTS\ex2000 to the Administrators local group on EXCH-PDC.
18. Gave ACCOUNTS\ex2000 "Logon Locally, Logon as a Service, Act as part of the Operating System and Restore Files and Directories" permissions to EXCH-BDC.
19. Ran SECEDIT /refreshpolicy MACHINE_POLICY and SECEDIT /refreshpolicy USER_POLICY. Exchange services would not start. I checked the event log and it said that SA couldn't start because a dependent service didn't start. It turns out that the RPC Locator service was somehow disabled during the demotion and move to ACCOUNTS. We enabled the RPC service and then all the Exchange services started.
20. Last step is to move all the EXCHANGE resource domain servers (EXCH-PDC, EXCH-BDC, CONN01, etc.) from the Computers container into an OU called Exchange in the ACCOUNTS domain.

Summary—Collapsing an Exchange Resource Domain

Everything appears to work after our initial conversion. But I still recommend avoiding this altogether and waiting for Exchange 2000, which does not rely on domain-based service accounts, as does Exchange 5.5. Using this logic, we could have just upgraded the EXCHANGE domain to Windows 2000, upgraded the Exchange servers to the Active-Directory-aware version and moved them into the ACCOUNTS domain. Once they were all relocated it would just be a matter of running DCPROMO on the EXCHANGE DC to demote it to a member server and reassigning it to a different domain, effectively eliminating the EXCHANGE child domain.

Collapsing resource domains to reclaim servers is a lot of work and involves great risk. Rule of thumb: to justify the effort, you should get back one server for every five Exchange servers you move. If I haven’t scared you away yet, here are the highlights from our upgrade:

- Back up all Exchange servers before beginning and make sure you can restore them.
- If the PDC and all the BDCs in the Exchange Resource domain are also Exchange servers, add another BDC to the domain, promote it to the PDC, and leave it around after the last Exchange server is removed so you can always roll back in case of emergency. Once that PDC is gone you will have to reinstall Exchange if you get locked out of the Exchange Administrator program.
- Make sure Exchange services are starting with the account you expect them to. When you change 10 service accounts and passwords per Exchange server, it’s easy to make a mistake.
- If you use override accounts on X.400 or Site connectors, be sure that you also modify the connection account.
- Make sure that the Exchange service account has all the rights it needs to the member servers running Exchange. By default only “Logon as a Service” is assigned when changing the account name. You also need “Act as part of the operating system” and “Restore files and directories” rights and local Administrator group membership.
- If you have any mailboxes with a Primary Windows NT account from the resource domain, you will have to change them to a valid account after moving the Exchange server into the new domain.
- If you have OWA configured, be sure to add the *IUSR_ServerName* account to the Configuration container and assign it Admin permissions.